REMARKS

Claims 1 – 33 are pending in the application. Claims 1 – 33 have been rejected. Claims 1 - 2, 12, 14 - 15, 22, 24 – 25, 28 - 29 and 33 have been amended. Claims 1 – 33 remain in the application and are presented for reconsideration. A new abstract is being submitted to overcome the examiner's objection to the length of the original abstract.

The Examiner rejected claims 1 – 11, 14 – 21, 24 – 28 and 30 – 33 under 35 USC § 102(e) as being anticipated by *Ballard*, U.S. Patent No. 6,032,137. This rejection is respectfully traversed. Anticipation under 35 USC § 102 requires the presence in a single prior art reference of each and every element in the claim, arranged in the claim.

Ballard teaches a remote image capture system with centralized processing and storage. The image capture system taught by *Ballard* processes paper and/or electronic receipts such as credit card receipts, ATM receipts, business expense receipts, and sales receipts, and automatically generates reports such as credit card statements, bank statements, tax reports for tax return preparation, market analyses, etc. (col. 3, ll. 37 – 42, 59 – 64).

The system taught by *Ballard* is a three tiered system including: DATs 200 that retrieve data from the customer (i.e., merchant) sites; system access collectors (DACs 400), which is the intermediate data collecting subsystem; and DPC 600, which polls the DACs 400 to retrieve accumulated data. This is not a teaching of a real time electronic transaction verification system. *Ballard* teaches polling and batch processing of data retrieved from data access terminals; therefore, *Ballard* teaches away from a real time electronic transaction verification system. The

DPCs 600 store the customer's data in a central location, generate reports from the data, and transmit the reports to the customers at remote locations. Customers represent credit card companies or transaction merchants. As shown in Fig. 3A of *Ballard* and as taught at col. 7, l. 59 – col. 9, l. 17, the system access terminal (DAT) scanner 202 scans paper receipts into the DAT 200 provided by an operator in step 310. In step 312, the DAT controller determines whether the operation executed successfully. If the scanning is successful, the DAT scanner 202 produces a bitmap image of the paper receipts. The DAT controller 210 executes a conventional image compression algorithm to compress the bitmap image in step 314. In step 316, the DAT controller 210 determines whether the compression executed successfully. If the compression is successful, a compressed bitmap image is produced. The compressed bitmap image is encrypted in step 318. If the encryption is successful, an encrypted compressed bitmap image of the scanned credit slips is created. The DAT controller 210 tags the encrypted compressed bitmap image with a time stamp that includes the scanning time, and an identification number to identify the merchant originating the scan in step 322. If the tagging is successful, a tagged encrypted compressed bitmap image is produced (TECBI). The TECBI is stored in the DAT digital storage 208 in step 326. The DAT controller 210 determines whether all paper receipts have been scanned in step 330. If all paper receipts have been scanned, the DAT controller 210 ask the operator to verify the number of scanned receipts in step 334. If the number of scanned receipts as determined by the DAT controller 210 equals the number of scanned receipts as determined by the operator, the DAT controller 210 prints a batch ticket on the DAT printer 206 in step 350.

Fig. 3B displays a sample paper receipt that is processed by the DAT 200 as described by the flowchart in Fig. 3A. The entire process described in the flowchart Fig. 3A involves batch processing of scanned paper receipts, i.e., the process occurs after the transactions have been completed and the paper receipts are available.

Ballard further teaches, at col. 14, ll. 19 – 33, that the DAC server 402 initiates the polling and data transmission at optimum poll rate times to decrease the cost of data transmission. As the DAT 200 polling and data transmission progresses, the system access controller (DAC) 400 will periodically update the DPC 600 with its status.

Claims 1, 14, 24, and 28 have been amended to indicate that both the identity of the individual presenting the transaction token and verification of a condition of a user account are performed in real time, i.e., in order to complete the transaction at the point-of-sale. Support for this amendment is found in paragraph 36 and in the processing logic of Fig. 3. Claims 1, 14 and 28 have also been amended to clarify that the reading device is reading information from the transaction token. Support for this amendment is provided in Figs. 1 – 2 and para. 30, ll. 19 –20.

With respect to claim 1, *Ballard* fails to teach a transaction information database for storing account information for an authorized user. In Applicant's invention, an authorized user is an individual authorized to use the electronic transaction verification system. An authorized user can be the account owner, i.e., the person having account information stored in a transaction information database and corresponding biometric data stored in a biometric database. An authorized user can also be the payee of a check, a subsequent payee or any other individual

authorized to access an account in the system. In *Ballard*, the customer is a vendor or a credit card merchant, not the authorized user or individual presenting a transaction token at a transaction location. *Ballard* teaches the storing of receipts, not account information for an authorized user. The receipts that are electronically stored are picked up periodically (polled) by the DAC.

Furthermore, *Ballard* fails to teach an electronic transaction verification system for use at a location where a transaction token is presented, in which the reading device selectively transmits transaction information data to the information database for comparison with the account information stored for the authorized user to verify a condition of the account in real time. Furthermore, there is no teaching in *Ballard* of a biometric data device selectively transmitting biometric data to a biometric database for comparison with biometric data stored for an authorized user to verify the identity of the individual presenting the transaction token in real time. Therefore, claim 1 is not anticipated by *Ballard*. Claims 14, 24 and 28 have similar limitations to those of claim 1. Therefore, claims 14, 24, and 28 are not anticipated by *Ballard*.

Claim 2 – 11 depend directly or indirectly from claim 1; claims 15 – 21 depend directly or indirectly from claim 14; claims 25 – 27 depend directly from claim 24; and claims 30 – 33 depend directly or indirectly from claim 28. Since the base claims are not anticipated, the dependent claims also are not anticipated by *Ballard*.

Claims 2, 15, 25 and 33 have been amended to recite that the transmitted signature data is compared with the signature stored for the authorized user in the signature database in real time.

Support for this amendment is provided in Fig. 1, block 22; Fig. 4, block 68; and para. 32, ll. 16 –20.

With respect to claim 2, *Ballard* teaches at col. 5, ll. 62 – 63, that DAT scanner 202 is capable of capturing handwritten signatures for identity verification. This is not a teaching of verifying the signature of an individual presenting a token in real time. Therefore, claim 2 is not anticipated by *Ballard* for this additional reason. The same argument applies to claims 15, 25 and 33, which recite the same limitations and are thus not anticipated by *Ballard* for this additional reason.

With respect to claims 3 and 16, *Ballard* teaches, at col. 6, ll. 37 – 47, the retrieval of identification information from the card itself for subsequent transmission to the destination of the internet transaction. There is no teaching in *Ballard* that transaction information is read electronically from the transaction token to determine, in real-time, the condition of an account stored in an electronic transaction database for an authorized user. Furthermore, the anonymous smart card taught by *Ballard,* at col. 17, lines 7 – 17, does not identify a user at all. Therefore, the transaction token in Applicant's invention is functionally different than the cards taught by *Ballard.*

With respect to claim 5, *Ballard* teaches at col. 22, ll. 22 – 30, that an electronic transaction representing a check is transmitted to the payee bank. See also, Fig. 10, logic blocks 1014 and 1016. This is not a teaching of transmitting transaction information data to a transaction information database as part of an electronic transaction verification system wherein

the transaction information data includes data written in magnetic ink on the check. Therefore, claim 5 is not anticipated by *Ballard* for this additional reason. Claim 17 recites the same limitation and is not anticipated by *Ballard* for the same reasons.

With respect to claim 6, *Ballard* teaches at col. 5, l. 52 – col. 6, l. 2, that DAT scanner 202 scans a paper receipt and generates a digital bitmap image representation of the receipt. In addition to scanning images and text, the DAT scanner also scans DataGlyph elements. In other words, the scanned paper receipt that is collected from a transaction location by a DAT 200 also scans DataGlyph elements on the receipt. The paper receipt captured by *Ballard* is not a teaching that transaction information data includes data encoded on the transaction token as recited in claim 6. Therefore, claim 6 is not anticipated by *Ballard* for this additional reason. Claim 18 recites a similar limitations to claim 6 and is not anticipated by *Ballard* for the same reasons.

With respect to claim 7, *Ballard* teaches at col. 6, l. 58 – col. 7, l. 3, that the DAT card interface 212 can read transaction data from a smart card that has been lost, stolen, damaged, or deliberately altered in order to reproduce the transaction data for the customer (i.e., merchant). The DAT card interface 212 provides support for independent verification of records maintained by consumers, merchants, and bankers to prevent a loss of data. This is not a teaching of selectively returning a report on customer usages by an electronic transaction verification system as recited in claim 7. Therefore, claim 7 is not anticipated by *Ballard* for this additional reason. Claim 19 recites a similar limitation and is not anticipated for the same reasons.

With respect to claim 8, *Ballard* teaches, at col. 6, ll. 53 – 58 and col. 7, ll. 41 – 44, that DATs 200 can include additional devices for capturing other biometric data for additional security. These devices include facial scans, fingerprints, voice prints, iris scans, retina scans, and hand geometry. *Ballard* further teaches that DAT controller 210 compresses, encrypts, and tags the bitmap image of a receipt to form a tagged encrypted compressed bitmap image (TECBI). These teachings of *Ballard* do not constitute a teaching of selectively encoding recorded biometric data on the transaction token as recited in claim 8. A transaction token is presented by an individual at the transaction location. It is not a paper or electronic receipt generated as a result of the transaction. Therefore, claim 8 is not anticipated by *Ballard* for this additional reason. Claims 20, 26 and 31 recite similar limitations and are not anticipated for the same reasons.

The Examiner rejected claims 12 – 13, 22 – 23, 29 and 32 under 35 USC § 103(a) as being unpatentable over *Ballard* in view of *Hoffman, et. al.*, U.S. Patent No. 5,613,012. This rejection is respectfully traversed. Applicant incorporates by reference the remarks made above for distinguishing claim 1 from the teachings of *Ballard*. *Hoffman* teaches at col. 69, ll. 54 – 65 that individuals are added to the system during an enrollment process in which individuals select their personal identification numbers and add financial asset accounts to their biometric and PIC combination. Individuals may be removed from the database due to fraudulent activity reported by any issuing member. If this occurs, the individual's account information is moved from the individual biometric database to the prior fraud database by an authorized internal systems

representative. The biometric IDs for records in the prior fraud database may not be used for records in the individual biometric database. Furthermore, at col. 71, ll. 34 – 42, *Hoffman* teaches that the prior fraud database is a collection of records representing individuals who have defrauded member issuers at some point in the past. The prior fraud database runs background transactions during periods of low system activity to weed out individuals in the individual biometric database who have matching records in the prior fraud database. This system does not automatically put individuals into a prior fraud database, unless it detects that they are attempting to register again.

Claims 12, 22 and 29 have been amended to recite that the additional biometric database automatically stores biometric data for a plurality of invalid users. Support for this amendment can be found at para. 11, ll. 1 – 10; para. 30, ll. 5 – 9; para. 34, ll. 8 – 10 and para. 43, ll. 7 – 18 of Applicant's specification. Therefore, claims 12, 22 and 29 are patentable over the combination of *Ballard* and *Hoffman, et al.* Moreover, these teachings of *Hoffman, et al.* do not represent a teaching of transmitting biometric data at the transaction location to the additional biometric database to determine if the individual presenting the transaction token is an invalid user as recited in claim 13. Therefore, claim 13 is patentable over the combination of *Ballard* and *Hoffman, et al.* Claims 23 and 32 recite a similar limitation as recited in claim 13 and are also patentable over the combination of *Ballard* and *Hoffman, et al.* for at least the same reason.

The prior art made of record has been reviewed, but is not deemed pertinent to Applicant's invention. None of the references cited teaches or suggests an electronic transaction

verification system in which the identity of the individual presenting a transaction token and a condition of an authorized user's account are verified in real time as recited in the claims.

In view of the above, it is submitted that the objection and rejections of the Examiner have been properly addressed and the pending claims are in condition for allowance. Such action at an early date is earnestly solicited. It is also requested that the Examiner contact Applicants' attorney at the telephone number listed below should this response not be deemed to place this application in condition for allowance.

Respectfully submitted,

5/11/05
Date

John J. Timar
Registration No. 32,497
Attorney for Applicants

Womble Carlyle Sandridge & Rice, PLLC
P.O. Box 7037
Atlanta, GA 30357-0037
(404) 888-7412 (Telephone)
(404) 870-2405 (Facsimile)